

Commuting probabilities of finite groups

Sean Eberhard

ABSTRACT

The commuting probability of a finite group is defined to be the probability that two randomly chosen group elements commute. Let $\mathcal{P} \subset (0, 1]$ be the set of commuting probabilities of all finite groups. We prove that every point of \mathcal{P} is nearly an Egyptian fraction of bounded complexity. As a corollary we deduce two conjectures of Keith Joseph from 1977: all limit points of \mathcal{P} are rational, and \mathcal{P} is well ordered by $>$. We also prove analogous theorems for bilinear maps of abelian groups.

Contents

1. Introduction	1
2. Neumann's theorem amplified	3
3. The main theorem	7
4. Joseph's conjectures	9
5. The order type of \mathcal{P}	10
References	13

1. Introduction

Suppose we measure the abelianness of a finite group G by counting the number of pairs of elements of G which commute. Call

$$\Pr(G) = \mathbf{P}_{x,y \in G}(xy = yx) = \frac{1}{|G|^2} |\{(x, y) \in G^2 : xy = yx\}|$$

the *commuting probability* of G . Then a possibly surprising first observation is that a group G with $\Pr(G) \approx 1$ must actually satisfy $\Pr(G) = 1$. In fact if $\Pr(G) < 1$ then $\Pr(G) \leq 5/8$. After such an observation it is natural to wonder what the rest of the set

$$\mathcal{P} = \{\Pr(G) : G \text{ a finite group}\}$$

looks like. For instance, is there some $\varepsilon > 0$ such that if $\Pr(G) < 5/8$ then $\Pr(G) \leq 5/8 - \varepsilon$? Is there some interval in which \mathcal{P} is dense? These sorts of questions were first studied in general by Keith Joseph [Jos69, Jos77], who made the following three conjectures.

CONJECTURE 1.1 Joseph's conjectures.

- J1. All limit points of \mathcal{P} are rational.
- J2. \mathcal{P} is well ordered by $>$.
- J3. $\{0\} \cup \mathcal{P}$ is closed.

Note that conjectures J1 and J2, if true, answer our questions above about the structure of \mathcal{P} , for J1 implies that \mathcal{P} is nowhere dense, and J2 implies that to every $p \in \mathcal{P}$ we can associate some $\varepsilon > 0$ such that $(p - \varepsilon, p) \cap \mathcal{P} = \emptyset$. Progress on J1 and J2 has been slow, however. The best partial result to date is due to Hegarty [Heg13], who proved that J1 and J2 hold for the set $\mathcal{P} \cap (2/9, 1]$.

From Hegarty's work one can begin to see a connection between commuting probability and so-called Egyptian fractions. The purpose of the present paper is to further develop this connection, and to use it to prove J1 and J2.

Define the *Egyptian complexity* $\mathcal{E}(q)$ of a rational number $q > 0$ to be the least positive integer m such that q can be written as a sum of reciprocals

$$q = 1/n_1 + \cdots + 1/n_m,$$

with each n_i a positive integer, agreeing that $\mathcal{E}(0) = 0$ and that $\mathcal{E}(x) = \infty$ if x is irrational. We prove the following structure theorem for the values of $\text{Pr}(G)$, which roughly asserts that commuting probabilities are nearly Egyptian fractions of bounded complexity.

THEOREM 1.2. *For every decreasing function $\eta : \mathbf{N} \rightarrow (0, 1)$ there is some $M = M(\eta) \in \mathbf{N}$ such that every commuting probability $\text{Pr}(G)$ has the form $q + \varepsilon$, where $\mathcal{E}(q) \leq M$ and $0 \leq \varepsilon \leq \eta(\mathcal{E}(q))$.*

COROLLARY 1.3. *All limit points of \mathcal{P} are rational, and \mathcal{P} is well ordered by $>$.*

We also prove a version of the above theorem for bilinear maps, partly as a model problem and partly for independent interest. Given finite abelian groups A, B, C and a bilinear map $\phi : A \times B \rightarrow C$, let

$$\text{Pr}(\phi) = \mathbf{P}_{a \in A, b \in B}(\phi(a, b) = 0) = \frac{1}{|A||B|} |\{(a, b) \in A \times B : \phi(a, b) = 0\}|.$$

Let \mathcal{P}_b be the set of all $\text{Pr}(\phi)$, where ϕ is such a bilinear map.

THEOREM 1.4. *For every decreasing function $\eta : \mathbf{N} \rightarrow (0, 1)$ there is some $M = M(\eta) \in \mathbf{N}$ such that every bilinear zero probability $\text{Pr}(\phi)$ has the form $q + \varepsilon$, where $\mathcal{E}(q) \leq M$ and $0 \leq \varepsilon \leq \eta(\mathcal{E}(q))$.*

COROLLARY 1.5. *All limit points of \mathcal{P}_b are rational, and \mathcal{P}_b is well ordered by $>$.*

The proofs of Theorems 1.2 and 1.4 rely on a theorem of Neumann [Neu89] which states that if a group G is statistically close to abelian in the sense that $\text{Pr}(G)$ is bounded away from 0 then G is structurally close to abelian in the sense that G has a large abelian section. We prove an amplified version of this theorem in Section 2 and we use it to deduce Theorems 1.2 and 1.4 in Section 3. We deduce Joseph's conjectures J1 and J2 in Section 4.

Assuming J2 holds, Joseph also asked for the order type of $(\mathcal{P}, >)$. We consider this question in Section 5. By examining the proof of Theorem 1.2 we reduce the number of possibilities for the order type to two.

THEOREM 1.6. *The order type of $(\mathcal{P}, >)$ is either ω^ω or ω^{ω^2} .*

The same theorem holds for \mathcal{P}_b .

2. Neumann's theorem amplified

LEMMA 2.1. *Let G be a finite group and X a symmetric subset of G containing the identity. Then $\langle X \rangle = X^{3r}$ provided $(r+1)|X| > |G|$.*

Proof. Suppose $x_i \in X^{3i+1} \setminus X^{3i}$ for each $i = 0, \dots, r$. Then for each i we have

$$x_i X \subset X^{3i+2} \setminus X^{3i-1},$$

so $x_0 X, \dots, x_r X$ are disjoint subsets of G each of size $|X|$, so

$$(r+1)|X| \leq |G|.$$

Thus if $(r+1)|X| > |G|$ we must have $X^{3i+1} = X^{3i}$ for some $i \leq r$, so we must have $\langle X \rangle = X^{3i} = X^{3r}$. \square

For $\phi : A \times B \rightarrow C$ a bilinear map and $A' \leq A$ and $B' \leq B$ subgroups, we denote by $\phi(A', B')$ the group generated by the values $\phi(a', b')$ with $a' \in A'$, $b' \in B'$.

THEOREM 2.2 (Neumann's theorem for bilinear maps). *Let $\varepsilon > 0$, and let $\phi : A \times B \rightarrow C$ be a bilinear map of finite abelian groups such that $\Pr(\phi) \geq \varepsilon$. Then there are subgroups $A' \leq A$ and $B' \leq B$ such that $|A/A'|$, $|B/B'|$ and $|\phi(A', B')|$ are each ε -bounded.*

Proof. Let $X \subset A$ be the set of $x \in A$ such that $|\ker \phi(x, \cdot)| \geq (\varepsilon/2)|B|$, and let A' be the group generated by X . Then $|X| \geq (\varepsilon/2)|A|$, so A' has index at most $2/\varepsilon$ in A , and by the lemma every $a \in A'$ is a sum of at most $6/\varepsilon$ elements of X , so for every $a \in A'$ we have $|\ker \phi(a, \cdot)| \geq (\varepsilon/2)^{6/\varepsilon}|B|$. Similarly, there is a subgroup B' of B of index at most $2/\varepsilon$ such that for every $b \in B'$ we have $|\ker \phi(\cdot, b)| \geq (\varepsilon/2)^{6/\varepsilon}|A|$. Then for every $a \in A'$ the subgroup $\ker \phi(a, \cdot) \cap B'$ has index at most $(2/\varepsilon)^{6/\varepsilon}$ in B' and for every $b \in B'$ the subgroup $\ker \phi(\cdot, b) \cap A'$ has index at most $(2/\varepsilon)^{6/\varepsilon}$ in A' .

Now consider any value c of ϕ on $A' \times B'$, say $c = \phi(a, b)$. If we replace a by any element a' of $a + (\ker \phi(\cdot, b) \cap A')$ and then b by any element b' of $b + (\ker \phi(a', \cdot) \cap B')$ then we still have $\phi(a', b') = c$, so

$$|\{(a', b') \in A' \times B' : \phi(a', b') = c\}| \geq (\varepsilon/2)^{12/\varepsilon} |A'| |B'|,$$

so ϕ takes at most $(2/\varepsilon)^{12/\varepsilon}$ different values on $A' \times B'$. But every element of $\phi(A', B')$ is a sum of distinct values of ϕ on $A' \times B'$, since if say

$$c = \sum_{i=1}^m \phi(a_i, b_i)$$

with the term $\phi(a_j, b_j)$ appearing twice then we can reduce the total number of terms by replacing $\phi(a_j, b_j) + \phi(a_j, b_j)$ with $\phi(2a_j, b_j)$. Thus $|\phi(A', B')| \leq 2^{(2/\varepsilon)^{12/\varepsilon}}$. \square

We need a stronger variant of the above theorem which asserts the existence of subgroups A' and B' such that (1) $\phi(A', B')$ is small and (2) $A' \times B'$ contains almost all pairs $(a, b) \in A \times B$

such that $\phi(a, b) \in \phi(A', B')$, in particular almost all pairs such that $\phi(a, b) = 0$. The precise formulation is the following.

THEOREM 2.3 (Neumann's theorem for bilinear maps, amplified). *For every decreasing function $\eta : \mathbf{N} \rightarrow (0, 1)$ there is some $M = M(\eta)$ such that the following holds. For every bilinear map $\phi : A \times B \rightarrow C$ there are subgroups $A' \leq A$ and $B' \leq B$ such that*

- (i) $|\phi(A', B')| \leq M$,
- (ii) *with at most $\eta(|\phi(A', B')|)|A||B|$ exceptions, every pair $(a, b) \in A \times B$ such that $\phi(a, b) \in \phi(A', B')$ is contained in $A' \times B'$.*

We have not stated a bound on $|A/A'|$ or $|B/B'|$, but such a bound is implicit if $\Pr(\phi) \geq \varepsilon$, since then

$$\varepsilon \leq \Pr(\phi) \leq \frac{1}{|A/A'||B/B'|} + \eta(|\phi(A', B')|).$$

Thus by ensuring $\eta(1) \leq \varepsilon/2$ one automatically has $|A/A'||B/B'| \leq 2\varepsilon^{-1}$.

Proof. If $\Pr(\phi) \leq \eta(1)$ then we can just take $A' = B' = \{0\}$, so assume otherwise. Then we can apply Theorem 2.2 with $\varepsilon = \eta(1)$. Let $A_1 \leq A$ and $B_1 \leq B$ be the resulting subgroups, let $C_1 = \phi(A_1, B_1)$, and suppose that more than $\eta(|C_1|)|A||B|$ pairs $(a, b) \in (A \times B) \setminus (A_1 \times B_1)$ satisfy $\phi(a, b) \in C_1$. Then there is some $(a, b) \in (A \times B) \setminus (A_1 \times B_1)$, say with $a \notin A_1$, such that at least $\eta(|C_1|)|A_1||B_1|$ pairs $(a', b') \in A_1 \times B_1$ satisfy

$$\phi(a + a', b + b') \in C_1,$$

or equivalently

$$\phi(a, b) + \phi(a, b') + \phi(a', b) \in C_1.$$

Then in particular for at least $\eta(|C_1|)|B_1|$ elements $b' \in B_1$ we must have

$$\phi(a, b') \in C_1.$$

But this implies

$$|(C_1 + \phi(a, B_1))/C_1| \leq \eta(|C_1|)^{-1},$$

so if we put $A_2 = A_1 + \langle a \rangle$, $B_2 = B_1$, $C_2 = \phi(A_2, B_2) = C_1 + \phi(a, B_1)$, then $|C_2| \leq \eta(|C_1|)^{-1}|C_1|$, $|B/B_2| \leq |B/B_1|$, and $|A/A_2| < |A/A_1|$. Now we can repeat the argument with A_2, B_2, C_2 in place of A_1, B_1, C_1 , but since $|A/A_1||B/B_1|$ is an $\eta(1)$ -bounded integer and $|A/A_2||B/B_2| < |A/A_1||B/B_1|$ this process must end after an $\eta(1)$ -bounded number of steps, at which time we will have the conclusion of the theorem. \square

We now turn our attention to the commutator map on groups, which behaves enough like a bilinear map for the above arguments to be emulated. In an arbitrary group G we write $[x, y]$ for the commutator $x^{-1}y^{-1}xy$ of two elements $x, y \in G$. We also write x^y for the conjugate $y^{-1}xy$, and we will use the relation $[x, y] = x^{-1}x^y$. For $H, K \leq G$ we write $[H, K]$ for the group generated by all commutators $[h, k]$ with $h \in H, k \in K$.

THEOREM 2.4 (Neumann's theorem). *Let $\varepsilon > 0$, and let G be a finite group such that $\Pr(G) \geq \varepsilon$. Then G has a normal 2-step nilpotent subgroup H of ε -bounded index such that $[[H, H]]$ is ε -bounded.*

Proof. Let $X \subset G$ be the set of all $x \in G$ such that $|C_G(x)| \geq (\varepsilon/2)|G|$, where $C_G(x)$ is the centraliser of x in G , and let K be the group generated by X . Then $|K| \geq (\varepsilon/2)|G|$, so K has index at most $2/\varepsilon$ in G , and by the lemma every $k \in K$ is the product of at most $6/\varepsilon$ elements of X , so for every $k \in K$ we have $|C_G(k)| \geq (\varepsilon/2)^{6/\varepsilon}|G|$. Thus also $|C_K(k)| \geq (\varepsilon/2)^{6/\varepsilon}|K|$.

Now consider a commutator $c = [x, y]$ of two elements $x, y \in K$. If we replace x by any element x' of $C_K(y)x$ and then y by any element y' of $C_K(x')y$ then we still have $[x', y'] = c$, so

$$|\{(x', y') \in K^2 : [x', y'] = c\}| \geq (\varepsilon/2)^{12/\varepsilon}|K|^2,$$

so there are at most $(2/\varepsilon)^{12/\varepsilon}$ distinct commutators of elements of K . Now a classical theorem of Schur (see [Rob96, 10.1.4]) implies that $|[K, K]|$ is ε -bounded.

To finish let $H = C_K([K, K])$. Then H has ε -bounded index in K , hence ε -bounded index in G , and since $[H, H] \subset [K, K]$ we see that H is 2-step nilpotent and $|[H, H]|$ is ε -bounded. \square

Now as in the case of bilinear maps we can prove a stronger variant which asserts the existence of a normal subgroup H such that $[H, H]$ is small and such that $H \times H$ contains almost all $(x, y) \in G \times G$ such that $[x, y] \in [H, H]$, in particular almost all commuting pairs. We will need the following generalisation of Schur's theorem due to Baer (see [Rob96, 14.5.2]).

LEMMA 2.5. *If M and N are normal subgroups of a group G then $|[M, N]|$ is bounded by a function of $|M/C_M(N)|$ and $|N/C_N(M)|$.*

THEOREM 2.6 (Neumann's theorem, amplified). *For every decreasing function $\eta : \mathbf{N} \rightarrow (0, 1)$ there is some $M = M(\eta)$ such that the following holds. Every finite group G has a normal subgroup H such that*

- (i) $|[H, H]| \leq M$,
- (ii) *with at most $\eta(|[H, H]|)|G|^2$ exceptions, every pair $(x, y) \in G^2$ such that $[x, y] \in [H, H]$ is contained in H^2 .*

Proof. If $\Pr(G) \leq \eta(1)$ then we can just take $H = 1$, so assume otherwise. Then we can apply Theorem 2.4 with $\varepsilon = \eta(1)$. Let $K_1 \leq G$ be the resulting subgroup, let $L_1 = K_1$, and suppose that more than $\eta(|[K_1, L_1]|)/2 \cdot |G|^2$ pairs $(x, y) \in G^2 \setminus (K_1 \times L_1)$ satisfy $[x, y] \in [K_1, L_1]$. Then there must be some $(x, y) \in G^2 \setminus (K_1 \times L_1)$, say with $x \notin K_1$, such that at least $\eta(|[K_1, L_1]|)/2 \cdot |K_1||L_1|$ pairs $(k, l) \in K_1 \times L_1$ satisfy

$$[xk, yl] \in [K_1, L_1].$$

By using the commutator expansion formula

$$[ab, cd] = [a, d]^b [b, d] [a, c]^{bd} [b, c]^d \quad (2.1)$$

and some further rearrangement, we can rewrite this as

$$[x, l^{-1}]^{-1} [x, y] [k^{-1}, y]^{-1} \in [K_1, L_1].$$

This implies that for some $l_0 \in L_1$ there are at least $\eta(|[K_1, L_1]|)/2 \cdot |L_1|$ elements $l \in L_1$ such that

$$[x, l^{-1}]^{-1} [x, l_0^{-1}] \in [K_1, L_1],$$

so for these l we have

$$[x, l_0^{-1}l] = ([x, l^{-1}]^{-1} [x, l_0^{-1}])^l \in [K_1, L_1].$$

Thus the subgroup $N_0 \leq L_1$ defined by

$$N_0 = \{l \in L_1 : [x, l] \in [K_1, L_1]\}$$

has index at most $2\eta(|[K_1, L_1]|)^{-1}$ in L_1 , thus index at most

$$2\eta(|[K_1, L_1]|)^{-1}|G/L_1|$$

in G . If N is the largest normal subgroup of G contained in N_0 then it follows that

$$|G/N| \leq (2\eta(|[K_1, L_1]|)^{-1}|G/L_1|)!$$

But note that if K_2 is the normal subgroup of G generated by K_1 and x then in fact

$$N = \{l \in L_1 : [K_2, l] \subset [K_1, L_1]\},$$

so

$$N/[K_1, L_1] = C_{L_1/[K_1, L_1]}(K_2/[K_1, L_1]).$$

Since trivially

$$K_1/[K_1, L_1] \leq C_{K_2/[K_1, L_1]}(L_1/[K_1, L_1]),$$

Lemma 2.5 implies that the size of

$$[K_2/[K_1, L_1], L_1/[K_1, L_1]] = [K_2, L_1]/[K_1, L_1]$$

is bounded by a function of $|L_1/N| \leq |G/N|$ and $|K_2/K_1| \leq |G/K_1|$, and thus the size of $[K_2, L_1]$ is bounded by a function of $\eta(|[K_1, L_1]|)$.

Now we can repeat the argument with K_2 and $L_2 = L_1$ in place of K_1 and L_1 , but since $|G/K_1||G/L_1|$ is an $\eta(1)$ -bounded integer and $|G/K_2||G/L_2| < |G/K_1||G/L_1|$ this process must end after an $\eta(1)$ -bounded number of steps, at which time we will have normal subgroups $K, L \leq G$ such that

- (i) $|[K, L]| \leq M$,
- (ii) with at most $\eta(|[K, L]|)/2 \cdot |G|^2$ exceptions, every pair $(x, y) \in G^2$ such that $[x, y] \in [K, L]$ is contained in $K \times L$.

But (ii) implies that with at most $\eta(|[K, L]|)|G|^2$ exceptions every pair $(x, y) \in G^2$ such that $[x, y] \in [K, L]$ is contained in both $K \times L$ and $L \times K$, and hence in $(K \cap L)^2$, so because

$$[K \cap L, K \cap L] \subset [K, L]$$

the conclusion of the theorem is satisfied by $H = K \cap L$. □

We pause to mention that Theorem 2.6 admits a rather clean formulation in terms of ultrafinite groups. Given a sequence of finite groups (G_n) and a nonprincipal ultrafilter $p \in \beta\mathbf{N} \setminus \mathbf{N}$, the set $\prod_{n \rightarrow p} G_n$ of all sequences $(g_n) \in \prod G_n$ defined up to p -almost-everywhere equality forms a group, which we refer to as an *ultrafinite group*. The properties of $G = \prod_{n \rightarrow p} G_n$ tend to reflect the asymptotic properties of (G_n) . A subset S of G is called *internal* if it is defined by subsets $S_n \subset G_n$ in the same way, namely if $(s_n) \in S$ if and only if $s_n \in S_n$ for p -almost-all n , in which case we write $S = \prod_{n \rightarrow p} S_n$. Internal subsets can be measured by assigning to $S = \prod_{n \rightarrow p} S_n$ the standard part of the ultralimit of $|S_n|/|G_n|$ as $n \rightarrow p$. The resulting premeasure extends to a countably additive measure, called *Loeb measure*, on the σ -algebra generated by the internal subsets. In this language Theorem 2.6 can be stated as follows.

THEOREM 2.7 (Neumann's theorem, amplified, ultrafinitary version). *Every ultrafinite group G has an internal normal subgroup H such that $[H, H]$ is finite and such that almost every pair $(x, y) \in G^2$ such that $[x, y] \in [H, H]$ is contained in H^2 .*

Given a subgroup $H \leq G$, let us temporarily refer to pairs $(x, y) \in G^2 \setminus H^2$ such that $[x, y] \in [H, H]$ as *bad pairs*. Then the theorem states that every ultrafinite group G has an internal normal subgroup H with finite commutator subgroup and almost no bad pairs.

Proof that Theorem 2.6 implies Theorem 2.7. Suppose G were an ultrafinite group such that every internal normal subgroup H with finitely many commutators has a positive measure set of bad pairs.

Note for every M there is some $\eta(M) > 0$ such that if $H \leq G$ is an internal normal subgroup with at most M distinct commutators then the set of bad pairs for H has measure at least $\eta(M)$. Indeed if not then for every k there is an internal normal subgroup $\prod_{n \rightarrow p} H_{n,k}$ with at most M distinct commutators and at most a measure $1/k$ set of bad pairs, so the internal normal subgroup $H = \prod_{n \rightarrow p} H_{n,n}$ has at most M distinct commutators and almost no bad pairs, contradicting our hypothesis about G .

Applying Theorem 2.6 then to G_n and $\eta/2$, we find normal subgroups $H_n \leq G_n$ with bounded-size commutator subgroups, say $|[H_n, H_n]| = M$ for p -almost-all n , such that H_n has at most $(\eta(|[H_n, H_n]|)/2)|G_n|^2$ bad pairs. But then $H = \prod_{n \rightarrow p} H_n$ has at most M commutators and at most a measure $\eta(M)/2$ set of bad pairs, a contradiction.

Thus for every ultrafinite group G there is an internal normal subgroup H with finitely many commutators and almost no bad pairs. By Schur's theorem $[H, H]$ is also finite. \square

Proof that Theorem 2.7 implies Theorem 2.6. If Theorem 2.6 failed then we would have some decreasing function $\eta : \mathbf{N} \rightarrow (0, 1)$ and for every n some finite group G_n such that every normal subgroup $H_n \leq G_n$ with $|[H_n, H_n]| \leq n$ has at least $\eta(|[H_n, H_n]|)|G_n|^2$ bad pairs. Let $G = \prod_{n \rightarrow p} G_n$. By Theorem 2.7 there is an internal normal subgroup $H = \prod_{n \rightarrow p} H_n$ of G with $[H, H]$ finite and almost no bad pairs. But then for p -almost-all n the group H_n has $|[H_n, H_n]| \leq |[H, H]| \leq n$ and fewer than $\eta(|[H, H]|)|G_n|^2$ bad pairs, a contradiction. \square

3. The main theorem

For an abelian group A we denote by \widehat{A} the group of characters $\gamma : A \rightarrow S^1$. Recall the size relation $|\widehat{A}| = |A|$ and the orthogonality relations

$$\begin{aligned} \mathbf{E}_{a \in A} \gamma(a) &= 1_{\gamma=1}, \\ \mathbf{E}_{\gamma \in \widehat{A}} \gamma(a) &= 1_{a=0}. \end{aligned}$$

LEMMA 3.1. *Let A, B, C be finite abelian groups and $\phi : A \times B \rightarrow C$ a bilinear map. Then $\mathcal{E}(\text{Pr}(\phi)) \leq |C|$.*

Proof. By orthogonality of characters we have

$$\begin{aligned} \text{Pr}(\phi) &= \mathbf{E}_{a \in A} \mathbf{E}_{b \in B} 1_{\phi(a,b)=0} \\ &= \mathbf{E}_{a \in A} \mathbf{E}_{b \in B} \mathbf{E}_{\gamma \in \widehat{C}} \gamma(\phi(a, b)) \\ &= \mathbf{E}_{a \in A} \mathbf{E}_{\gamma \in \widehat{C}} 1_{\gamma(\phi(a, B))=1} \\ &= \mathbf{E}_{\gamma \in \widehat{C}} \left(\frac{1}{|A|} |\{a \in A : \gamma(\phi(a, B)) = 1\}| \right). \end{aligned}$$

But for fixed $\gamma \in \widehat{C}$ the set $\{a \in A : \gamma(\phi(a, B)) = 1\}$ is a subgroup of A , so the above formula expresses $\text{Pr}(\phi)$ as a sum of $|C|$ terms of the form $1/n$ with n a positive integer. \square

Proof of Theorem 1.4. Fix $\eta : \mathbf{N} \rightarrow (0, 1)$ and $\phi : A \times B \rightarrow C$. Applying Theorem 2.3, we find some $M = M(\eta)$ and subgroups $A' \leq A$ and $B' \leq B$ such that $|\phi(A', B')| \leq M$ and such that no more than $\eta(|\phi(A', B')|)|A||B|$ pairs $(a, b) \in (A \times B) \setminus (A' \times B')$ satisfy $\phi(a, b) = 0$. Thus

$$\Pr(\phi) = \frac{1}{|A/A'| |B/B'|} \Pr(\phi_{A' \times B'}) + \varepsilon,$$

where

$$\mathcal{E}(\Pr(\phi_{A' \times B'})) \leq |\phi(A', B')| \leq M$$

by the lemma, and

$$\begin{aligned} \varepsilon &= \frac{|\{(a, b) \in (A \times B) \setminus (A' \times B') : \phi(a, b) = 0\}|}{|A||B|} \\ &\leq \eta(|\phi(A', B')|) \\ &\leq \eta(\mathcal{E}(\Pr(\phi_{A' \times B'}))). \end{aligned}$$

□

The proof of Theorem 1.2 is similar, but to prove a suitable analogue of Lemma 3.1 we need the following theorem of Hall [Hal56].

LEMMA 3.2. *In any group G the index of the second centre*

$$Z_2(G) = \{g \in G : [g, G] \subset Z(G)\}$$

is bounded by a function of $|[G, G]|$.

LEMMA 3.3. *Let G be a finite group. Then $\mathcal{E}(\Pr(G)) \leq |G/Z_2(G)| \cdot |[G, G]|$. In particular by Hall's theorem $\mathcal{E}(\Pr(G))$ is bounded by a function of $|[G, G]|$.*

Proof. Let A be the abelian group $[G, G] \cap Z(G)$, and let Z_2 be the second centre of G . Then by the orthogonality relations we have

$$\begin{aligned} \Pr(G) &= \mathbf{E}_{x \in G} \mathbf{E}_{y \in G} 1_{[x, y] = 1} \\ &= \mathbf{E}_{x \in G} \mathbf{E}_{y \in G} \mathbf{E}_{z \in Z_2} 1_{[x, yz] = 1} \\ &= \mathbf{E}_{x \in G} \mathbf{E}_{y \in G} \mathbf{E}_{z \in Z_2} \mathbf{E}_{\gamma \in \hat{A}} 1_{[x, yz] \in A} \gamma([x, yz]) \\ &= \mathbf{E}_{x \in G} \mathbf{E}_{y \in G} \mathbf{E}_{z \in Z_2} \mathbf{E}_{\gamma \in \hat{A}} 1_{[x, y] \in A} \gamma([x, yz]), \end{aligned}$$

since, by (2.1), $[x, yz] = [x, z][x, y]^z \in A$ if and only if $[x, y] \in A$. Moreover, if $[x, y] \in A$ then $[x, yz] = [x, z][x, y]$, so by orthogonality again we have

$$\begin{aligned} \Pr(G) &= \mathbf{E}_{x \in G} \mathbf{E}_{y \in G} \mathbf{E}_{z \in Z_2} \mathbf{E}_{\gamma \in \hat{A}} 1_{[x, y] \in A} \gamma([x, z]) \gamma([x, y]), \\ &= \mathbf{E}_{x \in G} \mathbf{E}_{y \in G} \mathbf{E}_{\gamma \in \hat{A}} 1_{[x, y] \in A} (\mathbf{E}_{z \in Z_2} \gamma([x, z])) \gamma([x, y]), \\ &= \mathbf{E}_{x \in G} \mathbf{E}_{y \in G} \mathbf{E}_{\gamma \in \hat{A}} 1_{[x, y] \in A} 1_{\gamma([x, Z_2]) = 1} \gamma([x, y]). \end{aligned}$$

For fixed $y \in G$, $\gamma \in \hat{A}$, let

$$G_{y, \gamma} = \{x \in G : [x, y] \in A, \gamma([x, Z_2]) = 1\}.$$

Then, again by (2.1), $G_{y,\gamma}$ is a subgroup of G and $x \mapsto [x, y]$ defines a homomorphism $G_{y,\gamma} \rightarrow A$, so

$$\Pr(G) = \mathbf{E}_{y \in G} \mathbf{E}_{\gamma \in \hat{A}} \frac{1}{|G/G_{y,\gamma}|} 1_{\gamma([G_{y,\gamma}, y])=1}.$$

Finally, the integrand here depends on y only through yZ_2 , so we can replace the expectation over $y \in G$ by an expectation over $yZ_2 \in G/Z_2$, so

$$\mathcal{E}(\Pr(G)) \leq |G/Z_2| \cdot |A| \leq |G/Z_2| \cdot |[G, G]].$$

□

Proof of Theorem 1.2. Fix $\eta : \mathbf{N} \rightarrow (0, 1)$ and G . By the lemma we can find another decreasing function $\eta' : \mathbf{N} \rightarrow (0, 1)$ such that

$$\eta'(|[G, G]|) \leq \eta(\mathcal{E}(\Pr(G)))$$

for all finite groups G . Applying Theorem 2.6 with η' , we find some $M = M(\eta)$ and a subgroup $H \leq G$ such that $|[H, H]| \leq M$ and such that no more than $\eta'(|[H, H]|)|G|^2$ pairs $(x, y) \in G^2 \setminus H^2$ satisfy $[x, y] = 1$. Thus

$$\Pr(G) = \frac{1}{|G/H|^2} \Pr(H) + \varepsilon,$$

where $\mathcal{E}(\Pr(H))$ is bounded by a function of $|[H, H]| \leq M$ by the lemma, and

$$\begin{aligned} \varepsilon &= \frac{|\{(x, y) \in G^2 \setminus H^2 : [x, y] = 1\}|}{|G|^2} \\ &\leq \eta'(|[H, H]|) \\ &\leq \eta(\mathcal{E}(\Pr(H))) \end{aligned}$$

by the choice of η' .

□

4. Joseph's conjectures

The following lemma is well known.

LEMMA 4.1. *For every $x > 0$ and $m \in \mathbf{N}$ the supremum of the set of $q < x$ such that $\mathcal{E}(q) \leq m$ is strictly less than x .*

Proof. Suppose for contradiction that n_{1i}, \dots, n_{mi} are m sequences of positive integers such that for all i

$$1/n_{1i} + \dots + 1/n_{mi} < x$$

and

$$1/n_{1i} + \dots + 1/n_{mi} \rightarrow x.$$

After rearranging and passing to a subsequence we may assume that $n_{1i} = n_1, \dots, n_{ki} = n_k$ are constants while $n_{k+1,i}, \dots, n_{mi} \rightarrow \infty$. But then

$$1/n_{1i} + \dots + 1/n_{mi} \rightarrow 1/n_1 + \dots + 1/n_k < x,$$

a contradiction.

□

Proof of Corollary 1.3. Let $x > 0$ be a limit point of $\mathcal{P} = \{\text{Pr}(G) : G \text{ a finite group}\}$. We will prove that x is rational, and that if $p_n \rightarrow x$ then $p_n \geq x$ for all but finitely many n .

For $m \in \mathbf{N}$ let

$$Q(m, x) = \sup\{q < x : \mathcal{E}(q) \leq m\}$$

and define

$$\eta_x(m) = (x - Q(m, x))/2.$$

By the lemma $\eta_x(m) > 0$ for every m , so by Theorem 1.2 there is some $M = M(\eta_x)$ such that every $p \in \mathcal{P}$ has the form $q + \varepsilon$, where $\mathcal{E}(q) \leq M$ and $0 \leq \varepsilon \leq \eta_x(\mathcal{E}(q))$.

Fix some such $p = q + \varepsilon$ and suppose $q < x$. Then

$$\varepsilon \leq \eta_x(\mathcal{E}(q)) \leq (x - q)/2,$$

so

$$p = q + \varepsilon \leq (q + x)/2 \leq (Q(M, x) + x)/2 = x - \eta_x(M),$$

so p is bounded away from x . Thus if $p_n = q_n + \varepsilon_n \rightarrow x$ then we must have $p_n \geq q_n \geq x$ for all but finitely many n . In particular $q_n \rightarrow x$, but the set of Egyptian fractions of complexity at most M is closed, so this implies $\mathcal{E}(x) \leq M$, so $x \in \mathbf{Q}$. \square

Corollary 1.5 is proved in exactly the same way.

5. The order type of \mathcal{P}

Having shown in previous sections that $(\mathcal{P}, >)$ is well ordered, we show in this final section that $(\mathcal{P}, >)$ has order type either ω^ω or ω^{ω^2} . First we need a standard definition.

For X a closed subset of $[0, 1]$ let $X' \subset X$ be the set of limit points of X . Iterating this operation, define X^α for ordinals α as follows:

$$\begin{aligned} X^0 &= X, \\ X^{\alpha+1} &= (X^\alpha)', \\ X^\alpha &= \bigcap_{\beta < \alpha} X^\beta \quad \text{if } \alpha \text{ is a limit ordinal.} \end{aligned}$$

If X is countable then there is a unique countable ordinal α for which X^α is finite and nonempty; we call α the *Cantor-Bendixson rank* of X . If X happens to be well ordered by $>$ then its order type is at most $\omega^\alpha + 1$, and if $X^\alpha = \{0\}$ and $\alpha > 0$ then in fact the order type of X is exactly $\omega^\alpha + 1$. (For a detailed introduction to Cantor-Bendixson rank see Dasgupta [Das14, Chapter 16].)

LEMMA 5.1. *Let X be a countably infinite closed subset of $[0, 1]$ closed under multiplication, and let α be the Cantor-Bendixson rank of X . Then $X^\alpha = \{0\}$ and $\alpha = \omega^\beta$ for some ordinal β .*

Proof. By induction on γ if $x \in X^\gamma$ and $y \in X$ and $y > 0$ then

$$xy \in X^\gamma.$$

Hence by induction on δ if $x \in X^\gamma$ and $x > 0$ and $y \in X^\delta$ and $y > 0$ then

$$xy \in X^{\gamma+\delta}.$$

Suppose $x \in X^\gamma$ and $x > 0$. Fix $y \in X \cap (0, 1)$. Then for all n we have

$$xy^n \in X^\gamma,$$

and $xy^n \rightarrow 0$, so

$$0 \in X^{\gamma+1}.$$

Hence we must have $X^\alpha = \{0\}$.

Now suppose $\gamma < \alpha$. Since $0 \in X^\alpha \subset X^{\gamma+1}$ there must be some $x \in X^\gamma \cap (0, 1)$. But then for all n we have

$$x^n \in X^{\gamma \cdot n},$$

so

$$0 \in X^{\gamma \cdot \omega}.$$

We deduce that

$$\alpha \geq \sup_{\gamma < \alpha} (\gamma \cdot \omega).$$

Let ω^β be the largest power of ω such that $\omega^\beta \leq \alpha$. If $\omega^\beta < \alpha$ then

$$\alpha \geq \sup_{\gamma < \alpha} (\gamma \cdot \omega) \geq \omega^\beta \cdot \omega = \omega^{\beta+1},$$

a contradiction, so we must have $\alpha = \omega^\beta$. □

Let $\overline{\mathcal{P}}$ be the closure of \mathcal{P} in $[0, 1]$. By the formula

$$\Pr(G \times H) = \Pr(G) \Pr(H)$$

we know that \mathcal{P} , and hence $\overline{\mathcal{P}}$, is closed under multiplication, so if α is the Cantor-Bendixson rank of $\overline{\mathcal{P}}$ then the lemma and the previous discussion implies that $\overline{\mathcal{P}}$ has order type $\omega^\alpha + 1$, so \mathcal{P} has order type ω^α , and moreover $\alpha = \omega^\beta$ for some β . Since for instance $1/2 \in \overline{\mathcal{P}}$ we know that $\beta > 0$. We will prove that $\alpha \leq \omega^2$, and thus $\alpha \in \{\omega, \omega^2\}$.

For $n \in \mathbf{N}$ let $\mathcal{E}_n = \{q : \mathcal{E}(q) \leq n\}$ be the set of Egyptian fractions of complexity at most n . The following lemma follows from the proofs of Theorem 1.2, Corollary 1.3, and Theorem 2.6.

LEMMA 5.2. *For every $\varepsilon_0 > 0$ there exist $k \in \mathbf{N}$ and a function $m : (0, 1] \rightarrow \mathbf{N}$ such that for all $\varepsilon_1, \dots, \varepsilon_k > 0$ the set*

$$\overline{\mathcal{P}} \cap [0, \varepsilon_0]^c \cap \bigcap_{i=0}^{k-1} (\mathcal{E}_{m(\varepsilon_i)} + [0, \varepsilon_{i+1}])^c$$

is finite.

Proof. Define $\eta_x(m) = (x - Q(m, x))/2$ as in the proof of Corollary 1.3. By inspecting the proofs of Theorem 1.2 and Theorem 2.6, we see that if $x > \varepsilon_0$ the constant $M = M(\eta_x)$ can be taken to be the result of iterating some function

$$t \mapsto b(\eta_x(h(t)))$$

some $n(\varepsilon_0)$ times starting with $n(\varepsilon_0)$, where

- $b : (0, 1] \rightarrow \mathbf{N}$ is a decreasing function coming from Baer's theorem (Lemma 2.5),
- $h : \mathbf{N} \rightarrow \mathbf{N}$ is an increasing function coming from Hall's theorem (Lemma 3.2),
- $n : (0, 1] \rightarrow \mathbf{N}$ is a decreasing function coming from Neumann's theorem (Theorem 2.4).

Let $k = n(\varepsilon_0) + 1$ and $m(\varepsilon) = \max(h(b(\varepsilon)), h(n(\varepsilon_0)))$, and suppose

$$x \in \mathcal{P} \cap [0, \varepsilon_0]^c \cap \bigcap_{i=0}^{k-1} (\mathcal{E}_{m(\varepsilon_i)} + [0, \varepsilon_{i+1}])^c. \quad (5.1)$$

Define the sequence t_0, t_1, \dots, t_k by

$$\begin{aligned} t_0 &= n(\varepsilon_0), \\ t_{i+1} &= b(\eta_x(h(t_i))) \quad \text{for } 0 \leq i < k. \end{aligned}$$

Then inductively

$$\begin{aligned} h(t_i) &\leq m(\varepsilon_i), \\ \eta_x(h(t_i)) &\geq \varepsilon_{i+1}, \\ t_{i+1} &\leq b(\varepsilon_{i+1}), \\ h(t_{i+1}) &\leq m(\varepsilon_{i+1}) \end{aligned}$$

for all i in the range $0 \leq i \leq k-1$, so

$$\eta_x(M) = \eta_x(t_{k-1}) \geq \eta_x(h(t_{k-1})) \geq \varepsilon_k.$$

But from the proof of Corollary 1.3 we know that

$$(x - \eta_x(M), x) \cap \mathcal{P} = \emptyset,$$

so there can be at most $1/\varepsilon_k$ elements x in the set (5.1), and the lemma follows. \square

Proof of Theorem 1.6. By the previous discussion it suffices to prove that $\alpha \leq \omega^2$. By the lemma we have

$$\overline{\mathcal{P}} \subset [0, \varepsilon_0] \cup \bigcup_{i=0}^{k-1} (\mathcal{E}_{m(\varepsilon_i)} + [0, \varepsilon_{i+1}]) \cup F$$

for some finite set F . From the rule $(X \cup Y)' = X' \cup Y'$ we have

$$\overline{\mathcal{P}}' \subset [0, \varepsilon_0] \cup \bigcup_{i=0}^{k-1} (\mathcal{E}_{m(\varepsilon_i)} + [0, \varepsilon_{i+1}]).$$

But since this holds for all $\varepsilon_k > 0$ we have

$$\overline{\mathcal{P}}' \subset [0, \varepsilon_0] \cup \bigcup_{i=0}^{k-2} (\mathcal{E}_{m(\varepsilon_i)} + [0, \varepsilon_{i+1}]) \cup \mathcal{E}_{m(\varepsilon_{k-1})}.$$

Now using $\mathcal{E}'_n = \mathcal{E}_{n-1}$ and the rule $(X \cup Y)' = X' \cup Y'$ again we have

$$\overline{\mathcal{P}}^{1+m(\varepsilon_{k-1})} \subset [0, \varepsilon_0] \cup \bigcup_{i=0}^{k-2} (\mathcal{E}_{m(\varepsilon_i)} + [0, \varepsilon_{i+1}]).$$

In particular

$$\overline{\mathcal{P}}^\omega \subset [0, \varepsilon_0] \cup \bigcup_{i=0}^{k-2} (\mathcal{E}_{m(\varepsilon_i)} + [0, \varepsilon_{i+1}]).$$

Repeating this argument another $k - 1$ times, we have

$$\begin{aligned}\overline{\mathcal{P}}^{\omega \cdot 2} &\subset [0, \varepsilon_0] \cup \bigcup_{i=0}^{k-3} (\mathcal{E}_{m(\varepsilon_i)} + [0, \varepsilon_{i+1}]), \\ &\vdots \\ \overline{\mathcal{P}}^{\omega \cdot (k-1)} &\subset [0, \varepsilon_0] \cup (\mathcal{E}_{m(\varepsilon_0)} + [0, \varepsilon_1]), \\ \overline{\mathcal{P}}^{\omega \cdot k} &\subset [0, \varepsilon_0].\end{aligned}$$

Thus

$$\overline{\mathcal{P}}^{\omega^2} \subset [0, \varepsilon_0]$$

for all $\varepsilon_0 > 0$, so

$$\overline{\mathcal{P}}^{\omega^2} \subset \{0\},$$

as claimed. \square

The same argument applies unchanged in the case of \mathcal{P}_b .

Acknowledgement. I thank Freddie Manners for the idea in the proof of Theorem 2.2 of bounding the size of $\phi(A', B')$ by showing that every value is taken many times, an idea which greatly simplified the proof.

References

- Das14** A. Dasgupta. *Set theory: with an introduction to real point sets*. Birkhäuser/Springer, New York, 2014.
- Hal56** P. Hall. Finite-by-nilpotent groups. *Proc. Cambridge Philos. Soc.*, 52:611–616, 1956.
- Heg13** P. Hegarty. Limit points in the range of the commuting probability function on finite groups. *J. Group Theory*, 16(2):235–247, 2013.
- Jos69** K. Joseph. *Commutativity in non-abelian groups*. PhD thesis, UCLA, 1969.
- Jos77** K. Joseph. Several conjectures on commutativity in algebraic structures. *Amer. Math. Monthly*, 84:550–551, 1977.
- Neu89** P. M. Neumann. Two combinatorial problems in group theory. *Bull. London Math. Soc.*, 21(5):456–458, 1989.
- Rob96** D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

Sean Eberhard
 Mathematical Institute
 Andrew Wiles Building
 Radcliffe Observatory Quarter
 Woodstock Road
 Oxford
 OX2 6GG
 UK
 eberhard@maths.ox.ac.uk